Joni Patrikainen

Mobile Network for Mass Events

Helsinki Metropolia University of Applied Sciences

Bachelor of Engineering

Information and Communication Technology

Thesis

30.10.2017

Helsinki Metropolia University of Applied Sciences

Author(s) Title Number of Pages Date	Joni Patrikainen Mobile Network for Mass Events 40 pages + 1 appendix 30 Aug 2017
Degree	Bachelor of Engineering
Degree Programme	Information and Communication Technology
Specialisation option	Communication networks and applications
Instructor(s)	Janne Salonen, Principal Lecturer

The purpose of this thesis was to create a network, which can transfer thermal images to a remote server from thermal cameras in heavily crowded events. The customer was keen on knowing if thermal cameras could be used to monitor audiences at music festivals. The network was tested practically at a music festival in 2017.

The planning and testing part of the thesis included hardware selection, device configuration and testing. In the networking solution, the data was transferred to a free mobile cell where it was transmitted through the 4G network and Internet to a server in another location.

The practical test part was arranged at a festival during August in 2017. The project was carried out in collaboration with another Metropolia student who designed the thermal cameras. The practical test revealed important information and during the test changes to the network were done to increase the performance.

As a result a video was combined from the images gathered from the weekend where crowd and people movement were visible. The biggest problem during the weekend was the connection between the thermal cameras and a WLAN access point. Even if the results did not fully meet the expectations the result of the practical test shows that thermal cameras can be used for audience monitoring at music festivals.

Keywords	WLAN, firewall, TCP/IP-model, 4G

Tekijä Otsikko Sivumäärä Päiväys	Joni Patrikainen Tietoverkko festivaalialueelle 40 sivua + 1 liite 30.10.2017
Tutkinto	Insinööri (AMK)
Tutkinto-ohjelma	Tieto- ja viestintätekniikka
Ammatillinen pääaine	Tietoverkot ja sovellukset
Ohjaaja	Yliopettaja Janne Salonen

Insinöörityön tarkoitus oli tehdä verkkoratkaisu, joka pystyy siirtämään lämpökameran kuvaamaa dataa palvelimelle. Verkkoratkaisun tulee toimia massatapahtumissa. Asiakas oli kiinnostunut tietämään, pystyykö lämpökameroita käyttämään festivaaliyleisön valvomiseen. Verkkoratkaisu testattiin festivaalilla vuonna 2017.

Suunnittelu- ja testausvaihe sisälsi laitteiston valitsemisen, konfiguroinnin ja testaamisen. Verkkoratkaisussa data siirrettiin vapaampaan mobiilisoluun, josta se lähetettiin 4G-verkon kautta Internettiin toisessa paikassa sijaitsevalle palvelimelle.

Käytännön testi järjestettiin festivaalin aikaan elokuussa 2017. Testin toteutettiin lämpökamerat suunnitelleen opiskelijan kanssa yhteistyönä. Testin aikana opittiin uutta ja tehtiin verkon suorituskykyä parantavia muutoksia.

Tulokseksi viikonlopun aikana kerätystä datasta työstettiin video, jonka kuvassa voi erottaa väkijoukot ja ihmisten liikkumisen. Suurimmaksi ongelmaksi osoittautui kameroiden ja tukiaseman välinen yhteys, johon pitää tehdä muutoksia mahdollisissa tulevissa käyttötarkoituksissa. Vaikka käytännön testin tulokset eivät olleetkaan odotettuja, ne osoittavat, että lämpökameroita voidaan käyttää yleisön valvontaan musiikkifestivaaleilla.

Avainsanat	WLAN, palomuuri, TCP/IP-malli, 4G

Contents

List of Abbreviations

IP	Internet Protocol
TCP	Transport Control Protocol
IOT	Internet of Things
PDU	Protocol Data Unit
DARPA	Defense Advanced Research Projects Agency
OSI	Open Systems Interconnection
MAC	Media Access Control
ARP	Address Resolution Protocol
TTL	Time To Live
NAT	Network Address Translation
UDP	User Datagram Protocol
WLAN	Wireless Local Area Network
DFS	Dynamic Frequency Selection
CSMA/CA	Carrier Sense Multiple Access With Collision Avoidance
RTS	Request to Send
CTS	Clear to Send
DHCP	Dynamic Host Configuration Protocol
ISP	Internet Service Provider
HTTP	Hypertext Transfer Protocol
FTP	File Transfer Protocol
ICMP	Internet Control Message Protocol
VPN	Virtual Private Network
eNodeB	Evolded NodeB
SGW	Serving Gateway
PGW	Packet Data Network Gateway
WiMAX	Worldwide Interoperability for Microwave Access
PoE	Power over Ethernet
LTE	Long Term Evolution
SSID	Service Set Identifier

1 Introduction

The purpose of this thesis was to plan and test a network which works in heavily crowded big events. The network should not depend on existing wired networks and it needs to be deployable in multiple locations. The thesis covers how networking was executed in an event where usually 4G networks are jammed due to the number of people in a small area.

The thesis is part of the project, which analyses how thermal cameras can be used for security applications. The customers were Flow Festival organizers who wanted to know whether thermal images could be used for monitoring purposes in big events. The thesis reports about requirement meetings, planning and a practical test. In addition, the thesis goes through the hardware configuration and theory behind the used networking methods.

To reach the goals set for the project the networking environment had to be planned and set up for the Flow Festival in August. The network transferred captured image data over the 4G network to the server. At the end of the thesis suggestions are given for how the networking can be improved for future events.

The employer for this project was Metropolia University of Applied Sciences. Metropolia collaborated with the rescue department and the Flow festival staff. Metropolia wanted to test the thermal cameras and research whether thermal cameras could be used in future projects and applications. Some applications are presented in Appendix 1.

This thesis contains 8 chapters: After the Introduction Chapter 2 focuses on explaining networking theory. Chapter 3 describes the events before the practical test. Chapter 4 focuses on explaining the configuration to the networking devices. Chapter 5 describes the events in the practical test. Chapter 6 shows the results of the project. Chapter 7 makes recommendations for improvements based on experience gained from the practical test. Chapter 8 provides the conclusions from the project.

2 Recent Theory on Data Transmission

This chapter explains crucial networking techniques used in the project starting from data transmitting to some more specific explanations of the techniques. For example, it explains general data transferring over the networks with TCP/IP-model and the packet capturing program Wireshark. Moreover, this chapter explains briefly different techniques used in the project.

2.1 Transmitting data through the networks

The main goal of this thesis was to move images from one place to another using networks. A network is devices connected to each other. Transmitting and receiving devices like computers, routers, switches and IoT devices are called nodes.

This chapter analyses one PDU captured from the firewall. PDUs are analyzed by using a packet capturing program called Wireshark. When thermal images move through the cameras to a server their movement on the network can be demonstrated with a 4-layer network model called Internet Protocol Suite or familiarly known as TCP/IP-model. It models the communication functions of a computing system. It was developed by DARPA and was published in 1974. Another way to model the communication functions is by using the OSI-model, which is a similar model to the 4-layer TCP/IP-model but it divides the fourth layer to three pieces. The firewall is the receiving end so the explanation is done in order from the first layer to the fourth. [1]

When transmitting data each layer encapsulates the data adding routing information needed to move it over the local network and the Internet. When the data arrives to its destination the receiving node needs to de-capsulate the information over the data. The data with the information is called PDU. PDU has a specific name on each layer of the TCP/IP-model. [2] The names are explained and demonstrated in Chapters 2.1.1-4.

All switches and routers on the way to receiving node does not encapsulate and de-capsulate. Basically, the encapsulation process is done on the transmitting node and de-capsulation process on the receiving node. PDUs are modified and some additional information may be added but the basic structure is done on the transmitter and the receiver.

2.1.1 Layer 1 - Network access layer

Layer 1 of the TCP/IP-model is called the network access layer. Layer 1 of the TCP/IP-model is called the network access layer. Layer 1 PDUs are called frames. [3] Figure 1 shows an image of the captured frame coming from Asus 4G router to Palo Alto firewall in the Wireshark.

Figure 1. Frame captured with the firewall showed in the Wireshark

In figure 1 the highlighted and collapsed part shows the structure of frame which includes destination and source MAC address and type. MAC addresses unify devices on the network and they are used as source (transmitter) and destination. (receiver) MAC address consists of six hexadecimal pairs. The first three pairs identify the device manufacturer. The rest of the pairs forms unique identifier for the device. Figure 1 also shows the size of the whole frame is 526 bytes. Layer 1 handles transmitting on the hardware level between the nodes. It also provides functionality for nodes on the same local network to transmit data between them. At the same local network means that nodes have an IP address from the same subnet and are behind the same router interface. When a node wants to send data through the network it first has to know where to send it to add a destination MAC address to the frame header. [4]

The node uses ARP protocol to find out if the receiving node is in the same local network. Figure 2 shows an image of ARP request (left) and ARP reply (right) created by Cisco Packet Tracer.

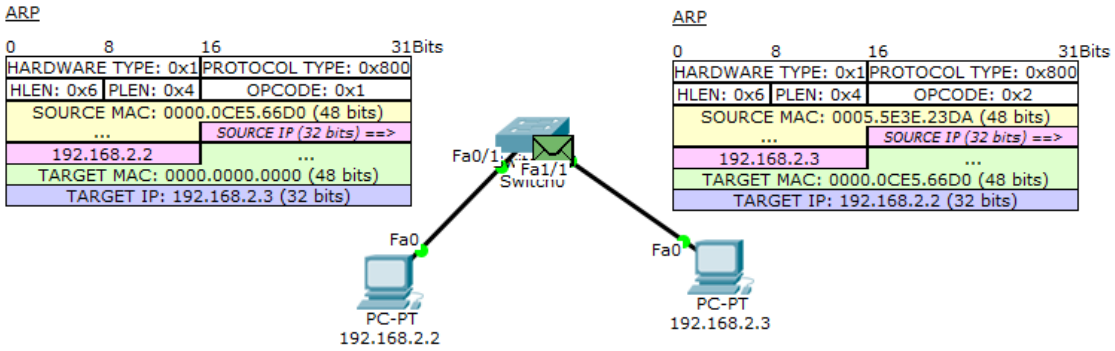


Figure 2. ARP request and reply created by Cisco Packet Tracer

In figure 2, a PC with IP address 192.168.2.2 asks which node has IP address 192.168.2.3 by sending an ARP request to every node on the local network. The PC with IP address 192.168.2.3 sends back ARP reply with its MAC address on it. Figure 3 shows the PCs ARP tables after the ARP request and response.

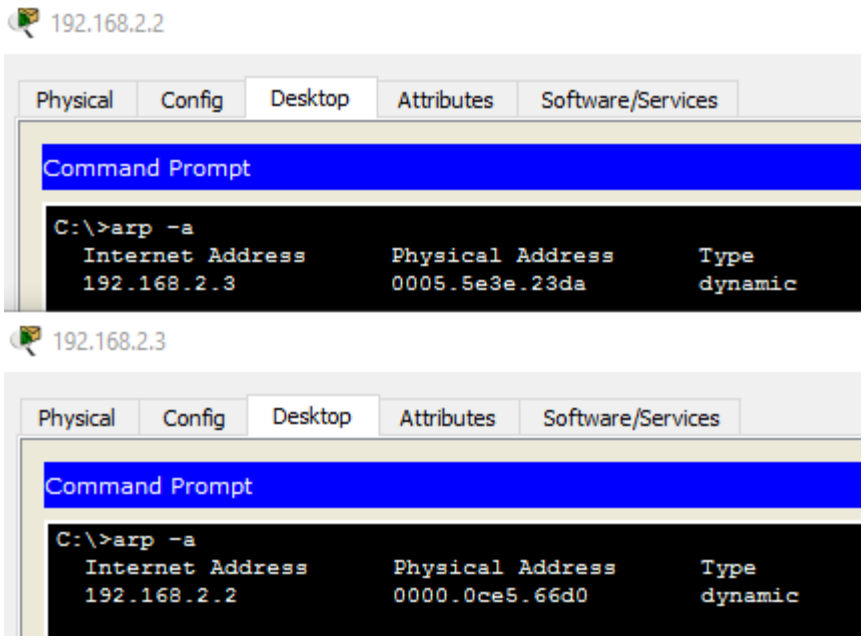


Figure 3. ARP table of PCs shown in Figure 2

In figure 3, the PCs has added their IP and MAC addresses to their ARP table. The node does not have to perform an ARP reply if it already has the destination MAC address on its ARP table. If the destination IP address is not on the same subnet the node has to send PDUs to it default gateway. The default gateway is usually the router on the edge of the local network. [5]

For example:
The thermal camera wants to send data to the server. The server is on other network. The thermal camera checks its ARP table finds its default gateway's MAC address. The thermal camera sends the encapsulated data to the default gateway which is the 4G router.

2.1.2 Layer 2 - Internet layer

Layer 2 of the TCP/IP-model is called the Internet layer. PDUs on the layer 2 are called packets. Routers uses packets to send the data to other networks. IP networks are called packet switched networks because core networks are mostly formed by routers and routes route packets. [6]

Routers have a list of known networks called a routing table. The router compares destination address of the packet to its routing table. If it finds a match from its routing table it checks the routing table entry to see where the router needs to send the PDU next. (Next hop address) Before sending it modifies its MAC address to source MAC address field found in the frame and the destination MAC address field to the next hop addresses MAC address. Router also decreases TTL value by one. When TTL value reaches zero the packet is not routed anymore and it is dropped. Figure 4 shows image of captured packet coming from the Asus 4G router to the Palo Alto firewall in the Wireshark. [7]

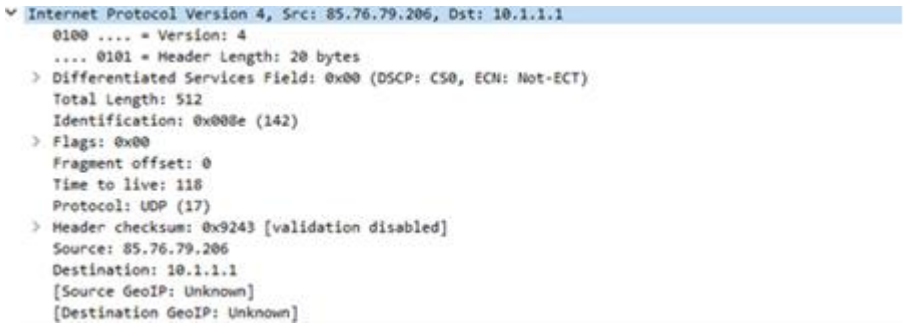


Figure 4. Packet captured with the firewall showed in the Wireshark

As shown in figure 4, the highlighted and collapsed part shows that data has come from 85.76.79.206 (Flow Festival site 4G router's address) and is going to 10.1.1.1. (Firewall local address) The reason why the firewall's address is local is because NAT was performed on the PDU. NAT is explained in Chapter 2.3.1.

2.1.3 Layer 3 - Transport layer

Layer 3 of the TCP/IP-model is called the transport layer. Layer 3 establishes, maintains and terminates connections between nodes. In the project layer 3 adds an UDP header in front of the data. When the UDP protocol is used PDUs on the layer 3 are called datagrams. [8, 9]

The camera modules are coded to use the UDP for data transfer. The UDP is a connectionless data transfer protocol which does not check if the data was sent correctly. The UDP is suited for applications which need fast and efficient data transmission. [9.]

Other protocol could have been used is TCP. Figure 5 shows TCP connection establishment and data transmission.

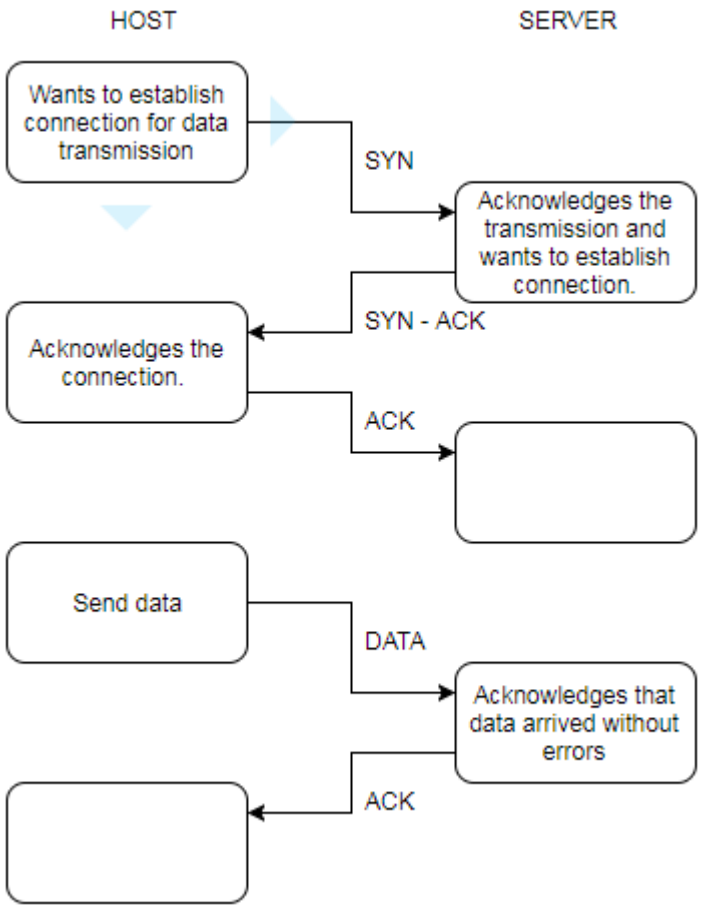


Figure 5. Procedure of the connection establishment of TCP

In figure 5, a host wants to access a website on a server. The process begins with the host sending a synchronize (SYN) message to the server. The server sends a synchronize---acknowledgement (SYN-ACK) message as an acknowledgement. The host sends an acknowledgement (ACK) message. The connection establishment is also known as three-way handshake. While sending data the receiver sends the acknowledgements (ACK) if the data arrived and does not have errors. If the transmitter doesn't receive the acknowledgement (ACK) it sends the data again. When the transmitter wants to terminate the connection, it does the same three-way handshake but the synchronize (SYN) messages are changes to a finish (FIN) messages. The TCP is suitable for applications which needs high reliability for cost of time. The UDP was chosen for the project because transmission needed to be as fast as possible. [10, 11]

The UDP protocol adds 8 bytes (8*8=64 bits) long header in front of the data. Figure 6 shows an image of captured UDP header coming from the Asus 4G router to the Palo Alto firewall in Wireshark. [12]

Figure 6. UDP header captured with the firewall showed in the Wireshark

Figure 6 shows that the UDP header consists of:

- Source port: Tells which port sent the PDU.
- Destination port: Tells which port received the PDU.
- Length: Tells how many bytes the UDP header + data is.
- Checksum: Checksum is UDP's error detection method. The receiver counts its own checksum and if it does not match to the header's checksum the PDU is dropped.

2.1.4 Layer 4 - Application layer

Layer 4 of the TCP/IP-model is called the application layer. The application layer handles data from an user interface to a network by forming the data to a format which is accepted by the receiving node. [13]

For example:

Image data is formed on the layer 4 and its size is coded to always be 484 bytes. In the project the program code in the cameras sends the data formed to the raw image format. Figure 7 shows an image of a protocol stack.

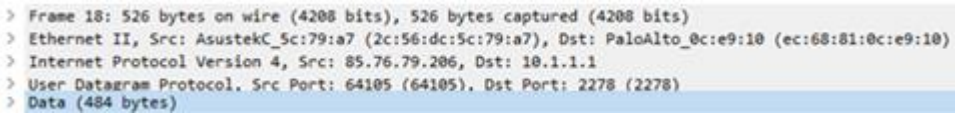


Figure 7. Protocol stack shown in the Wireshark

The stack in Figure 7 is the whole example analyzed in the Chapter 2.1. The destination node networking interface needs to do the de-capsulation process in order to get the data information out of the stack. In the examples showed in the Chapter 2 the destination seems to be the Palo Alto firewall but the Palo Alto firewall does not do the de-capsulation because it has been configured to port forward packets coming to the port 2278 to the server. Port forwarding is explained in Chapter 2.3.2.

2.2 WLAN

WLAN is used to connect nodes wirelessly to a network. WLAN was used to connect the thermal cameras to the network and to establish a link between directional antennas. WLAN operates on the 2.4GHz and the 5GHz bands. Figure 8 shows image of the band of the 2.4GHz WLAN.

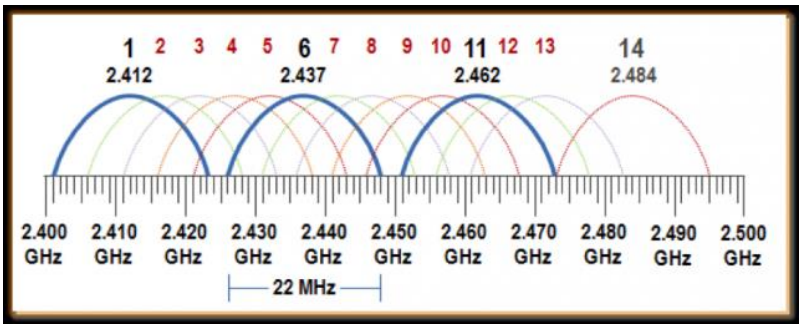


Figure 8. Band of 2.4GHz WLAN copied from lecture handout [14]

Curved lines in figure 8 are 22MHz blocks called channels. Commonly only 13 channels are used. The channel 14 is used only in Japan. The highlighted blue channels indicates the channels which does not overlap which each other. The non-overlapping channels (1, 6, 11) are preferred because there is fewer interferences than on the overlapping channels. [14.] In the project the 2.4GHz WLAN was used because the camera modules could not operate on the 5GHz band. The 2.4GHz band WLAN is not preferred because in cities the 2.4GHz band is heavily occupied.

Figure 9 shows image of the band of 5GHz WLAN.

Channel Number	Frequency MHz	Europe (ETSI)	North America (FCC)	Japan
36	5180	Indoors	✓	✓
40	5200	Indoors	✓	✓
44	5220	Indoors	✓	✓
48	5240	Indoors	✓	✓
52	5260	Indoors / DFS / TPC	DFS	DFS / TPC
56	5280	Indoors / DFS / TPC	DFS	DFS / TPC
60	5300	Indoors / DFS / TPC	DFS	DFS / TPC
64	5320	Indoors / DFS / TPC	DFS	DFS / TPC
100	5500	DFS / TPC	DFS	DFS / TPC
104	5520	DFS / TPC	DFS	DFS / TPC
108	5540	DFS / TPC	DFS	DFS / TPC
112	5560	DFS / TPC	DFS	DFS / TPC
116	5580	DFS / TPC	DFS	DFS / TPC
120	5600	DFS / TPC	No Access	DFS / TPC
124	5620	DFS / TPC	No Access	DFS / TPC
128	5640	DFS / TPC	No Access	DFS / TPC
132	5660	DFS / TPC	DFS	DFS / TPC
136	5680	DFS / TPC	DFS	DFS / TPC
140	5700	DFS / TPC	DFS	DFS / TPC
149	5745	SRD	✓	No Access
153	5765	SRD	✓	No Access
157	5785	SRD	✓	No Access
161	5805	SRD	✓	No Access
165	5825	SRD	✓	No Access

Figure 9. Band of 5GHz WLAN copied from lecture handout [14]

Figure 9 shows that the 5GHz band is divided to 20MHz channels and there is more than 20 non-overlapping channels. There is less traffic per channel than on the 2.4GHz band. In Europe wireless routers use commonly channels from 36 to 64 because DFS channels are used for radars and licensed devices. The DFS channels are also less populated so the project's directional antennas operated on these channels. In order to a non-licensed device to operate on the DFS channel it needs to scan the channel for 1-10 minute time period before transmitting on the channel. If the device detects traffic from for example a radar it must switch the channel. The only down site for the DFS channels is that after the scan if for example radar starts using the channel the non-licensed device has to

switch the channel and the connection is dropped for a time period of a new scan. Transmitting power in Finland is limited to 100mW/20dBm (2,4GHz) and 200mW/23dBm (5GHz). [14, 15]

Only a one node can transmit data to an access point/a router per time on WLAN network. The access point is a device on the network which provides wireless access to the network but it is not acting as a router. WLAN can use CSMA/CA method to avoid multiple devices transmitting on the same time. [14] Figure 10 shows operations of the CSMA/CA.

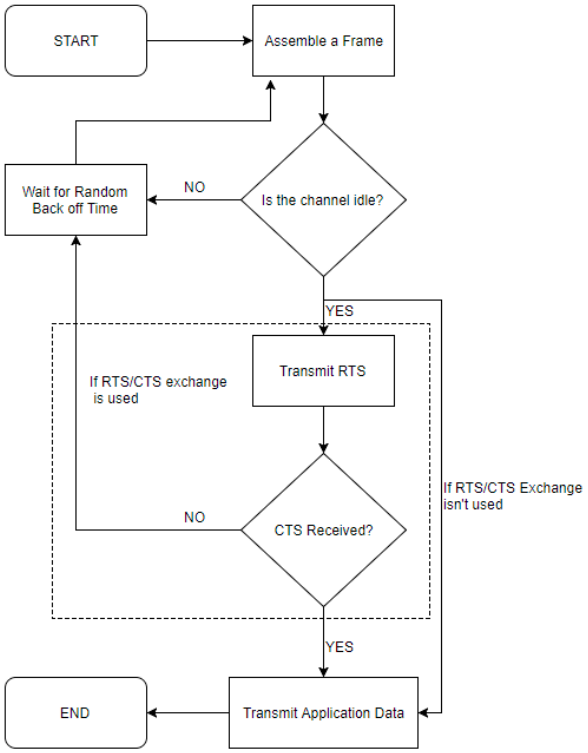


Figure 10. CSMA/CA procedure

Figure 10 shows that by default collisions are avoided by checking if the channel is in idle mode. If a device detects that the channel is not on the idle mode it can transmit data to the access point. If the device detects that the channel is not on the idle state it waits for a randomly chosen time before trying to send again.

The method described earlier is not effective if for example two devices are connected to the same access point and cannot hear each other.

Figure 11 shows image of hidden node problem. [14]

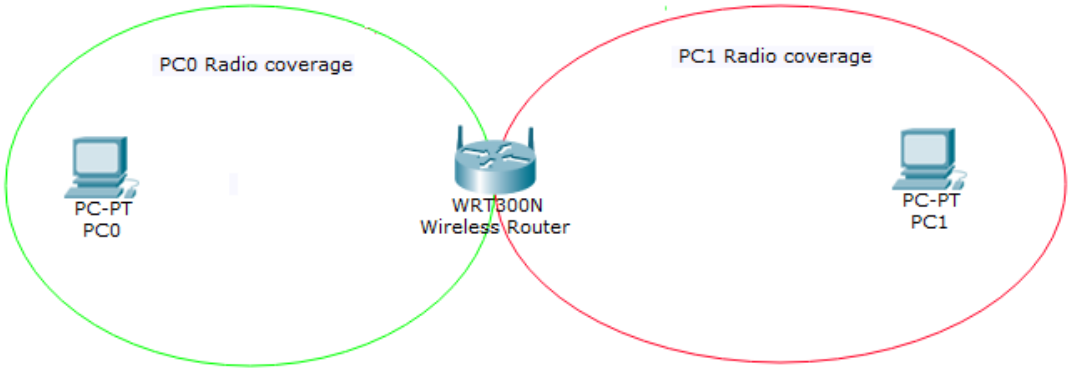


Figure 11. Hidden node problem

Figure 11 shows a situation where PC0 and PC1 are connected to the same access point but their radio coverage isn't big enough to detect the other device on the network. The solution for this is called RTS/CTS exchange. The RTS/CTS exchange is shown in Figure 10 in a dotted square. A node starts normally checking if the channel is in the idle mode. Then the node sends a RTS frame to the access point. The access point answers with a CTS frame. Then the node can transmit data to the access point. If the node detects that the channel is not on the idle mode or it does not receive the CTS frame it waits a randomly chosen time before trying to send again. In access points and WLAN routers the RTS/CTS exchange can be activated by reducing RTS/CTS threshold value. By default the value is often 2346. The value tells how big frames needs to go through the RTS/CTS mechanism. Because the max frame size on Ethernet network can be ~1500 bytes the RTS/CTS exchange is never used by default. By enabling the RTS/CTS exchange more frames move on the network which decreases the throughput of the network but in certain situation it is better to have smaller throughput versus corrupted frames by the collisions. [16] In the project the RTS/CTS exchange was enabled by changing the RTS threshold value to 0. The reason is explained in Chapter 5.3.

2.3 Firewalling and Routing

Firewall monitors traffic and blocks unauthorized traffic. The firewall is usually placed on the edge of a network to separate the Internet and a local network. The firewall in many situations acts also as a router. It performs router's tasks like NAT, port forwarding and maintaining a routing table.

2.3.1 NAT

NAT was developed as a temporary solution for the IPv4 because there isn't enough IPv4 addresses for every device on the Internet For example in a home environment a home router uses NAT to get one public IP address from the ISP and every device in home are seen with the public IP address given to the home router by the ISP. [17] Figure 12 shows the base line of an example of NAT.

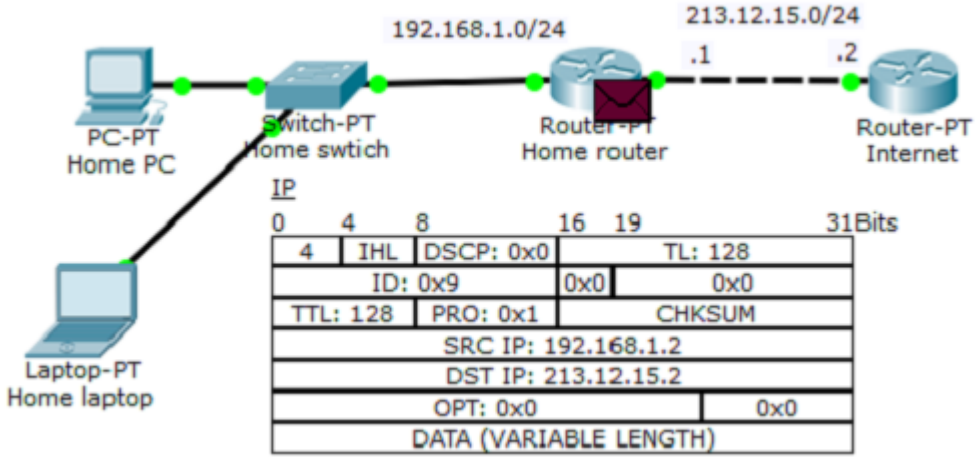


Figure 12. NAT example in Cisco Packet Tracer

In figure 12, the packet is going from the Home laptop to the Internet. The IP chart displays the information of the packet. Packets were explained in Chapter 2.1.2. The packet source is Home laptop's address 192.168.1.2 and the destination is some device in the Internet. 213.12.15.2. Figure 13 demonstrates the functionality of NAT.

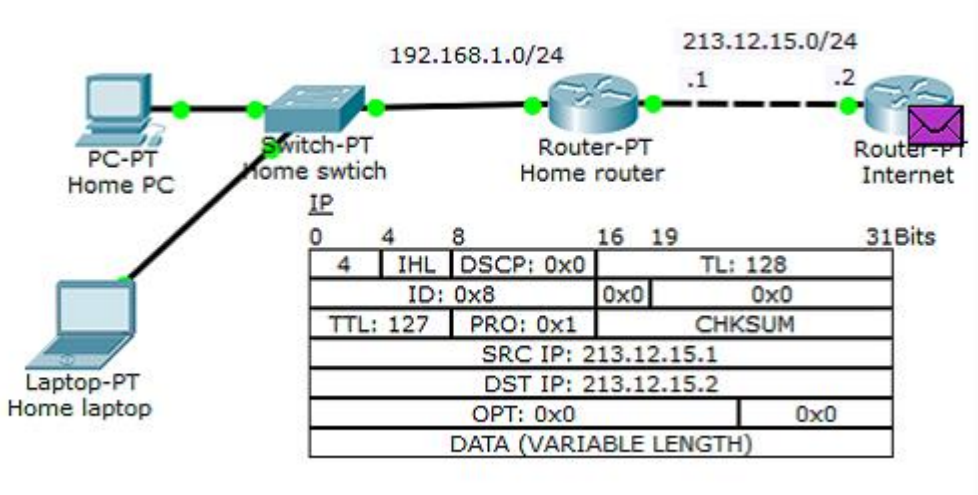


Figure 13. NAT functionality demonstrated in Cisco Packet Tracer

Figure 13 shows what happens to the packet when NAT is configured. The packet has been routed from the Home router to the Internet. The home router translates Home laptop's IP address to a public IP address assigned to the Home router via ISP's DHCP. Because of NAT the source IP (SRC IP) field contains the home router's public interface's IP address. [17] Figure 14 shows the same situation shown in Figure 13 but without using NAT.

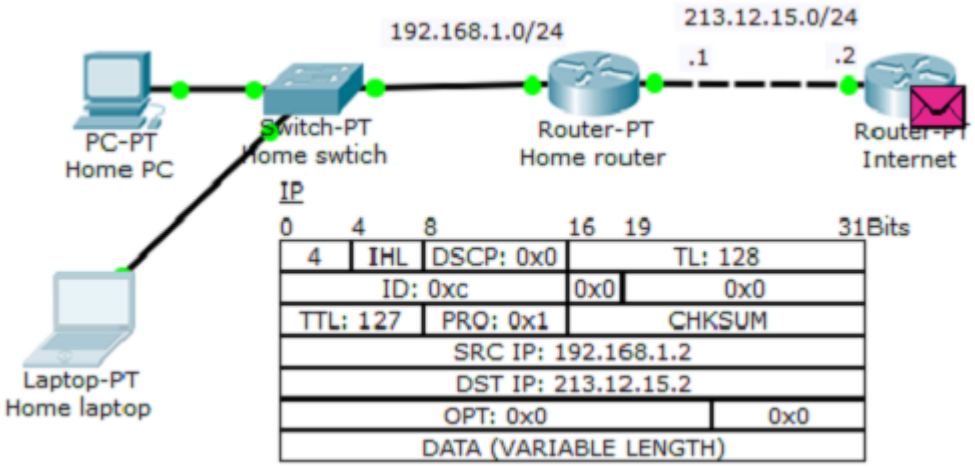


Figure 14. Figure 13 situation without NAT in Cisco Packet Tracer

In figure 14, the source address remains as it was on the local network. In a real world situation the packet is dropped between the routers in Figure 14 because ISP's router does not accept packets sourced from the local network's IP address.

2.3.2 Port forwarding

While using NAT, port forwarding can be used to redirect packets coming from a specific TCP/UDP-port to a predefined IP address. [18] Port forwarding was used in the project to forward UDP packets from the 4G router to the firewall. Pros using NAT with port forwarding are that many services can be reached from a one IP address. Figure 15 shows the base line of port forwarding example.

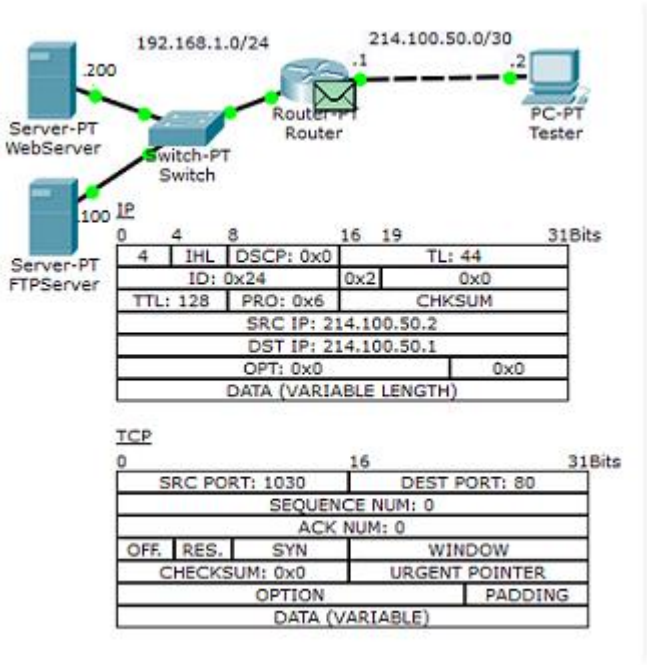


Figure 15. Port forward example shown in Cisco Packet Tracer

In figure 15, the packet is coming from the Tester to Router's public IP address 214.100.50.1 port 80 (HTTP). The packet holds a TCP header which tells the communication ports. The router determines the packet destination by using the port numbers. The router in figure 15 has NAT configured to route the packets coming to the port 80 to the WebServer. Figure 16 demonstrates port forwarding configuration of the router in figure 15.

```
ip nat inside source static tcp 192.168.1.100 21 214.100.50.1 21
ip nat inside source static tcp 192.168.1.200 80 214.100.50.1 80
                                LOCAL            PUBLIC
```

Figure 16. Port forwarding commands from the router in the example in figure 15

In figure 16, the squared IP address and port number sets are the most important. For example if a packet comes to the public address 214.100.50.1 port 80 (Figure 16 green square) the router know to forward the packet to the local IP address 192.168.1.200 (Figure 16 red square) which is the WebServer from figure 15. Figure 17 demonstrates the functionality of port forwarding. Without the commands shown in figure 16 the packet is dropped in the example shown in figure 15 because the router does not know what to do with HTTP or FTP packet.

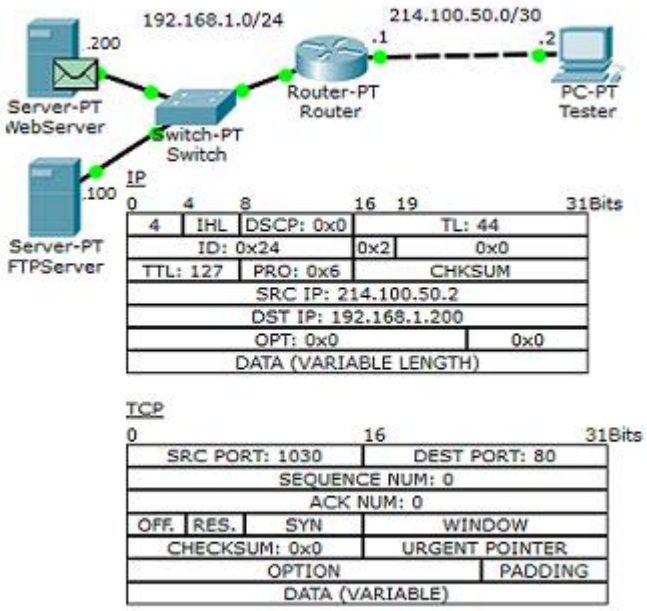


Figure 17. Port forwarding demonstrated in Cisco Packet Tracer

Figure 17 shows that the packet was directed to the WebServer with the IP address 192.168.1.200 because of the port forward commands shown in figure 16.

Figure 18 demonstrates what happens when Tester sent a FTP packet to the router.

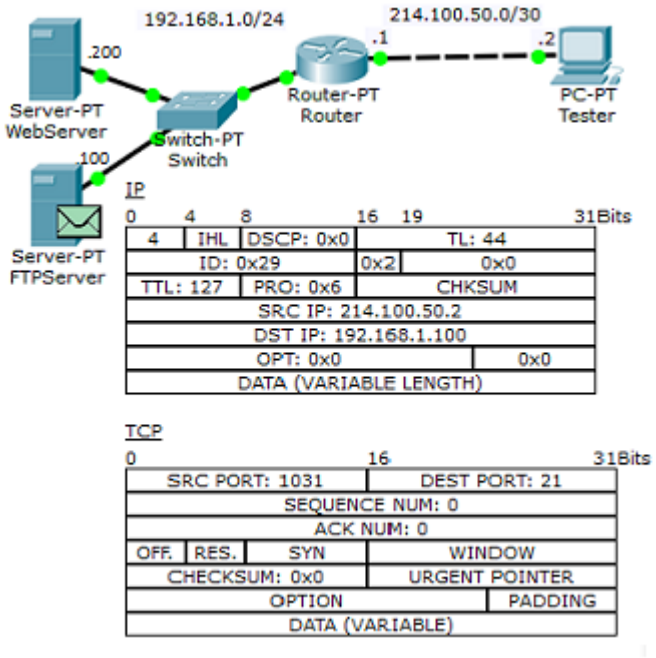


Figure 18. Figure 17 situation with a FTP packet

As depicted in figure 18, the router received a packet with the destination port 21. Router has the forward rule shown in figure 16 which tells the router to forward packets coming to the port 21 to 192.168.1.100 which is the FTPServer.

2.3.3 Access lists

Access lists are meant to deny or allow traffic in or out of a networking interface. [19] Access list is usually shortened to ACL. In the project, access lists are placed to the firewall to tell it what kind of traffic the firewall should allow to pass. The router on the port forwarding example showed in figures 15, 17 and 18 has also an access list configured which allows only traffic coming to 214.100.50.1 ports 21 (FTP) and 80. (HTTP)

Figure 19 demonstrates functionality of the ACL and shows the router configuration.

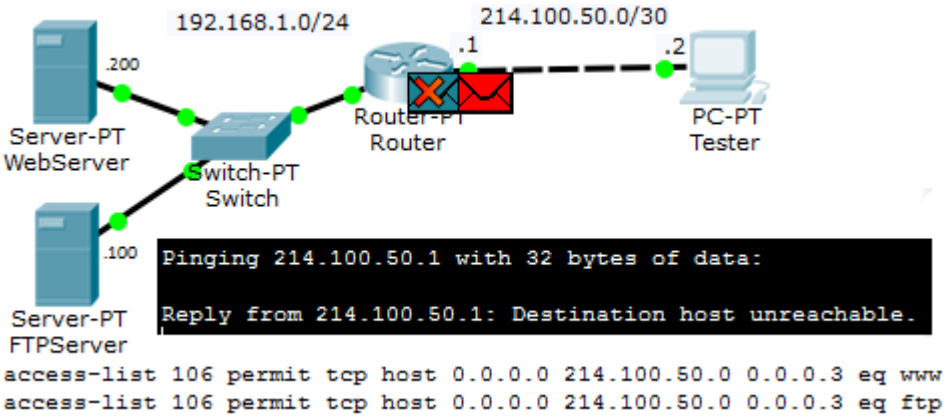


Figure 19. ACL demonstration and router commands in Cisco Packet Tracer

In figure 19, the Tester is trying to ping 214.100.50.1. The router denies the ICMP reply and sends back an administratively prohibited message which displays as “Destination host unreachable.” on Tester’s command-line interface. The bottom of figure 19 shows router's ACL commands. The commands tells to let any packet from any IP address (0.0.0.0) to access any IP address from IP address space 214.100.50.0/30 (214.100.50.1-2) when the port is equal to www (80) or FTP. (21)

2.3.4 VPN

VPN is used to create a private connection over the public network. VPN was used in the project to make a remote connection to the server which was used to store the data. A VPN performing router (in the project the firewall) encapsulates original PDU and encrypts it with for example a pre-shared key so only the destination router can encapsulate the packet. [20]

Figure 20 shows a situation where VPN is configured.

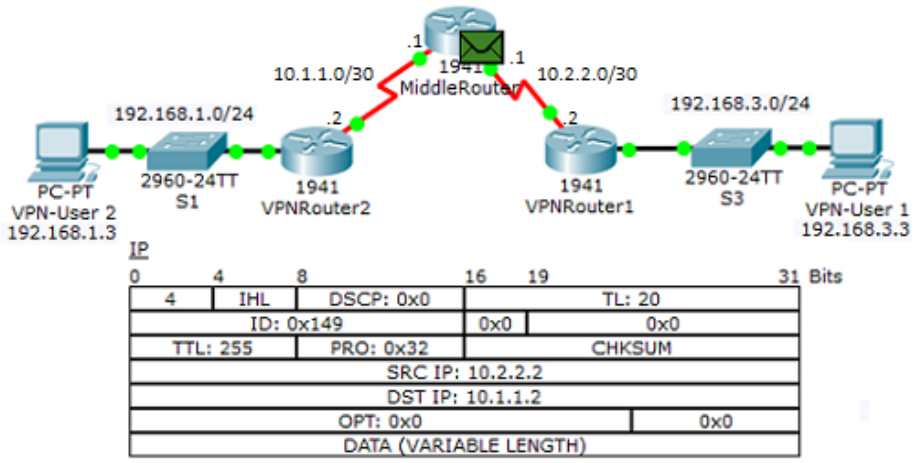


Figure 20. VPN demonstration in Cisco Packet Tracer

In figure 20, the MiddleRouter packet's source IP address is 10.2.2.2 (VPNRouter1's public networking interface) but the packet is sent from the VPN-User 1 because the VPNRouter1 is performing VPN encapsulation. Figure 21 shows the packets looks like when it went behind the VPNRouter2.

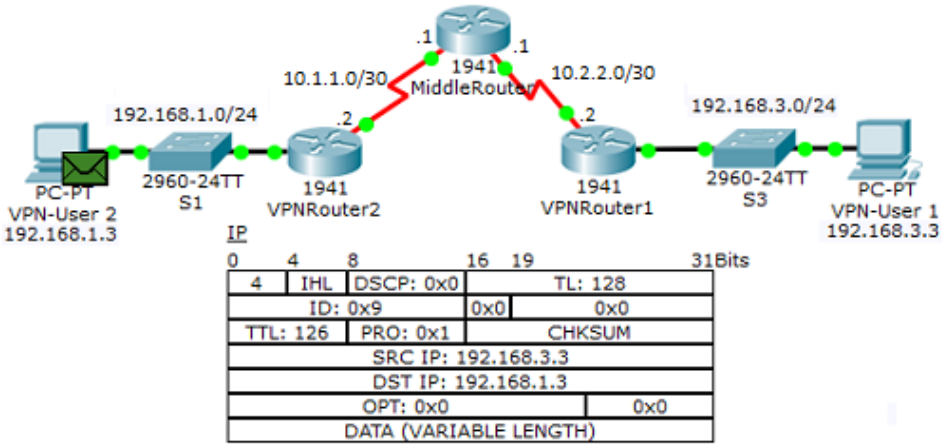


Figure 21. Packet inspection after VPNRouter2

In figure 21, the VPNRouter2 has performed VPN de-capsulation hence the packet's destination and source has changed to the original source and destination.

2.4 Cellular networks

Usually cellular networks are heavily occupied in big festivals. For example when trying to upload a picture to the Internet in a big music festival and it cannot be uploaded because the specific cellular cells on the festival area are so heavily occupied that their bandwidth can't handle all the customers. In order to send live images through the 4G network the 4G router needed to be on a different cell than the main festival area.

4G is as its name says 4th generation of cellular network technology. It is the first generation of the cellular network technology, which uses only packet switched networks which is explained on chapter 2.1. 4G offers fast data rates where the downlink rate exceed 100Mbits/s and the uplink rate exceeds 50Mbits/s with a latency between an user and a server on the Internet approximately 20ms. [21]

How does a packet go from the 4G router from the Flow Festival to the 4G router in Metropolia Leppävaara campus? When the 4G router connects to a cellular tower tower's communication building has to be equipment with an eNodeB which communicates with devices like 4G routers and mobile phones. The eNodeB sends packets to a SGW which routers and forwards packets to and from the eNodeB to a PGW. The PGW is the interface between the 4G network and other IP networks like ISP's core network and the Internet. [21]

3 Meetings, Planning and Testing

This chapter describes all the phases before the practical test. In particular, it describes the requirement meetings with different collaborators and how the actual hardware were chosen. Moreover, it describes tests carried out with directional antennas.

3.1 Meetings

There were several meetings before the practical test. The first meeting was held in March with the Flow Festival organizers and Metropolia's representatives. Metropolia presented the idea of using thermal cameras to get images from people behavior on the events without violating privacy terms. The Images could be used for example to monitor unusual behavior such people starting to avoid a certain spot with a small heat spot. One could assume that there could be a fight going on. Other example would be that if the area needs to be evacuated and people start to rush to a certain direction, the festival crew could check the thermal images to know which fences needs to be opened so that people does not get crushed to walls. The image data could be used by the rescue department and the event designers for planning future events. The idea was accepted and Metropolia got an initial permission to place the cameras in the Tuska and Flow Festival.

A couple of meetings were held with the rescue department and the Flow Festival security staff. The purpose was to discuss about safety and security. The rescue department representative presented about the fire safety and the safety rules operating in mass events. The representative also told to Metropolia's personnel where the rescue department wants to point the cameras. Metropolia needed to present the idea for the security personnel and get the permission to place the cameras. The Flow Festival security stated that the data is going to be sensitive and it needs to be handled safely without going to wrong hands. The Flow organizers did not want to give the data to public websites. The idea was to place the server behind a firewall and make it accessible only with a VPN connection. Metropolia got the permission to place the cameras and collect the data after the safety plans were presented.

Some smaller meetings were held with Metropolia's people to keep everyone updated what has been developed and what is in progress. The Tuska Festival denied Metropolia's access because their timetable was too busy to have other moving parts in the puzzle.

3.2 Planning

The requirements for the network was that it needs to be mobile and not depended on existing wired networks. Because of the requirements 4G was chosen to be the connection method to the Internet. . The idea was to move data from the heavily occupied cellular cell to another cell and then send it to the server. Options for moving the data from a cell area to an another cell area thought were WiMAX and WLAN. WiMAX was soon dropped out of plans because of its costs.

The data needed to be safely used and handled and the cameras could not store the data locally so there wasn't a local data saved in the festival area. The local data saving was not an option also because in the meetings it was mentioned that the data should be accessible during the festival. The data was planned sent through a site-to-site VPN tunnel over the 4G network to a server in Leppävaara campus. The server was planned to be placed to Leppävaara's campus. In the plans, the server is placed behind a firewall which secures the data and is used as a VPN terminal.

The first thing to get was the directional antennas for the link from Suvilahti to the 4G gateway router. After some time of researching Ubiquinti Nanobeam AC19 antennas were chosen because of their performance and cost efficiency. A directional antenna is an antenna type which focuses energy to a certain direction. The antennas are powered with an included PoE adapter and they were suited for outdoor use. The manufacturer promised that these antennas could connect to each other from over 15 kilometres. The maximum distance was not tested.

A 4G router needed to be reliable and intelligent enough to switch between connections if the main connection fail or comes back up. Cisco's enterprise level router Cisco 819 4G LTE M2M was suggested. The router has a 4G interface and a gigabit interface for the Internet connections. It would be suitable for future projects for Metropolia. The 4G router would be located on Agricolakatu's campus so the wired connection could have been set go through the Metropolia's network as a backup connection.

A Palo Alto PA-200 firewall was chosen because the firewall was part of a previous project and it was basic configured already. The firewall used Nokia's 4G network to connect to the Internet. Because the firewall did not have a 4G interface it had to be connected to the 4G router.

A server requirement was that it could hold around 200GB of images. One image is 76kB and the camera captures 8.8 per second. Images from 72 hours is 175GB of data. Metropolia offered a decent workstation for this role.

The plan was accepted except for the 4G router. The project did not have money for the Cisco router and Metropolia didn't have anything like the Cisco router already. Metropolia had a Cisco's 3G router hence the 3G router was configured for a test. Its maximum throughput was 4 Mbits/second with high latency. The 3G router was not good enough to be the primary connection. Metropolia gave Asus RT-AC56 for the project. The 3G router was tried to be configured as a secondary connection for the Asus 4G router but the 4G router didn't support routing in its LAN interface. So the secondary connection was left out because of costs and only the 4G was used for the connection between the Flow Festival and Leppävaara campus. The Site-to-site VPN could not be established because the Asus 4G router did not support it.
When the cameras were assembled they did not have wired network interfaces and did not support the 5GHz WLAN technology so the 2.4GHz WLAN technology had to be used to connect the cameras to the network. The project did not have money for a suitable access point so any access point available had to be used.

Hardware set up used for the network:

- Palo Alto PA-200 Firewall
- Asus 4G N12 LTE Router
- Cisco 2800 Switch
- Asus RT-56AC Router
- 2x Ubiquinti Nanobeam 5AC 19
- Netgear WNR1000v3 Wireless Router

3.3 Testing

The aspect causing most concern was whether the directional antennas could connect from greater distances with an acceptable latency.

Figure 22 shows the first test set up.

Figure 22. The first test of the directional antennas

In figure 22, the antennas are 50m from each other in the campus corridor. This test was passed clearly. Turning and twisting the antennas did not affect the connection in 50m distance.

The second test was also at the campus. The antennas were placed so that the signal had to through three walls. The connection was established but more precision was needed with directing.

The third test was to place the antennas where they were planned to be. Figure 23 shows the directional antenna placement on Google Maps.

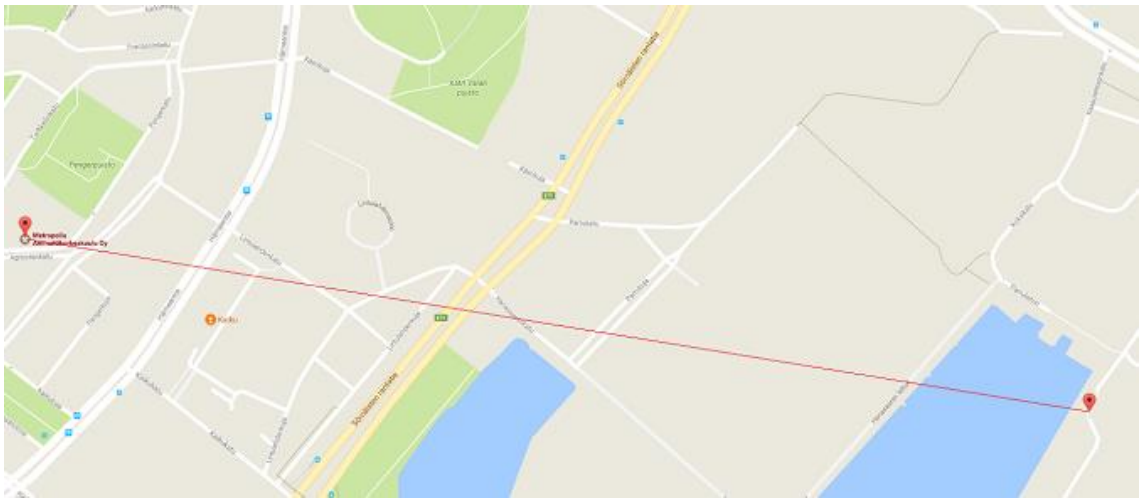


Figure 23. The directional antenna placement on Google Maps

In figure 23, the receiving antenna was placed to Metropolia's Agricolankatu campus. The campus is located 1.5 kilometers away from Suvilahti. On the test day there was no access to Suvilahti so the sending antenna was placed to Hernesaari (Figure 23) which is behind Suvilahti. Distance between these points was 1.8 kilometers. After a 10 minute DFS scan (Chapter 2.2) the connection was established even if the sending antenna was hand held to Agricolankatu's direction. Delay between the antennas was under 1 millisecond and directional antenna's graphical user interface showed that the throughput was around 300 Mbits/s.

The cameras were planned to install to a tower in front of the main stage. The tower height and installation options were checked a week before the festival. The tower was 16 meters high which was ideal for the cameras because optimally the cameras needed to be at least 10 meters above the ground. The networking plans faced an issue because there was a tall building blocking vision to Agricolankatu's campus. In a test the signal couldn't bend over the building.

The receiving antenna had to be moved to another location. Options were Korkeasaari and Katajanokka. The plan was to use Metropolia's "Nuuskija"-van which had large batteries on it and place the van to Korkeasaari or Katajanokka with the antenna. Korkeasaari was left out from options because there wasn't any parking spots which could have a line of sight to Suvilahti.

Figure 24 shows possible place for the van in Katajanokka.

Figure 24. Possible antenna alignment

In figure 24, the plan was to use Merikasarminkatu's free parking slots to park the van. In a test Helsingin Energia's building proved to be too large and it was blocking the signal. The final antenna placement is explained in Chapter 5.1.

4 Device configuration

This chapter briefs reader to device configurations on the network. Chapter 4.1 explains the essential firewall configurations for the project by showing examples from the firewall Palo Alto PA-200. Chapter 4.2 explains how the 4G routers were configured and shows examples from Leppävaara's 4G gateway router Asus 4G N12 LTE. Chapter 4.3 explains the configuration in the Ubiquinti Nanobeam AC19 directional antennas.

4.1 Palo alto PA-200

NAT

Figure 25 shows the NAT rules of the firewall.

	Name	Tags	Source Zone	Destination Zone	Destination Interface	Source Address	Destination Address	Service	Source Translation	Destination Translation
1	Inside to Outside	none	inside	outside	any	any	any	any	dynamic-ip-and-port ethernet1/1 10.1.1.1/24	none
2	BIMNAT	none	outside	outside	any	any	10.1.1.1	BIM-UDP	none	address: 192.168.100.101

Figure 25. NAT rules of the firewall.

In figure 25, Rule 2 is very important to the project because without it the server cannot receive the data from the cameras even if the other networks components are working properly. The rule transfers every packet's destination coming to outside interface's IP address 10.1.1.1 port 2278 to server's IP address 192.168.100.101 port 2278. The service column row 2 "BIM-UDP" is a defined service which indicates to the port 2278. Rule 1 changes firewall's local IP addresses into 4G router's IP address space so the 4G router knows to transfer addresses into the public IP address.

Port forwarding from the 4G router to the server cannot be done because the Asus 4G router cannot be configured to forward packets straight to other networks. In Figure 27, it can't be stated that everything coming to the UDP port 2278 is forwarded straight to 192.168.100.101. An interesting thing to notice was that the Palo Alto firewall does not port forward packets between its own interfaces hence NAT port forwarding had to be used. NAT and port forwarding were explained in Chapters 2.3.1 and 2.3.2.

Access list

Figure 26 shows the access lists of the Palo Alto PA-200 firewall.

				Source		Destination				
	Name	Tags	Type	Zone	Address	Zone	Address	Application	Service	Action
1	TO INTERNET	none	universal	[redacted] inside	any	outside	any	apt-get dns icmp paloalto-upd... panos-global... panos-web-i... ping more...	any	Allow
2	BIM UDP	none	universal	any	any	any	any	any	BIM-UDP	Allow
3	FROM INTERNET	none	universal	outside	any	inside	any	panos-global... panos-web-i... secure-access ssl teamviewer	any	Allow
4	intrazone-default	none	intrazone	any	any	(intrazone)	any	any	any	Allow
5	interzone-default	none	interzone	any	any	any	any	any	any	Deny

Figure 26. Access lists of the Palo Alto PA-200

In figure 26, Rule 2 allows the UDP port 2278 pass the firewall. The column "Address" had value "any" which was replaced with the public IP address of festival site. Palo Alto's networking interfaces are placed to zones. Public interface is called "outside" and local network zone is called "inside".

VPN

In order to get a VPN connection the firewall a VPN portal and a gateway had to be configured. The portal manages client connections giving the clients information about the gateway and certificates. The gateway provides a VPN access for the clients.

Before the portal can be configured the firewall has to have a tunnel interface configured. The tunnel interface does not need any configuration but it has to be created to interfaces. The tunnel interface is used to create a secure connection between the client and the firewall. (Example demonstrated in figure 20)

The portal configuration includes network and authentication settings. Figure 27 demonstrates the portal configuration on the firewall.

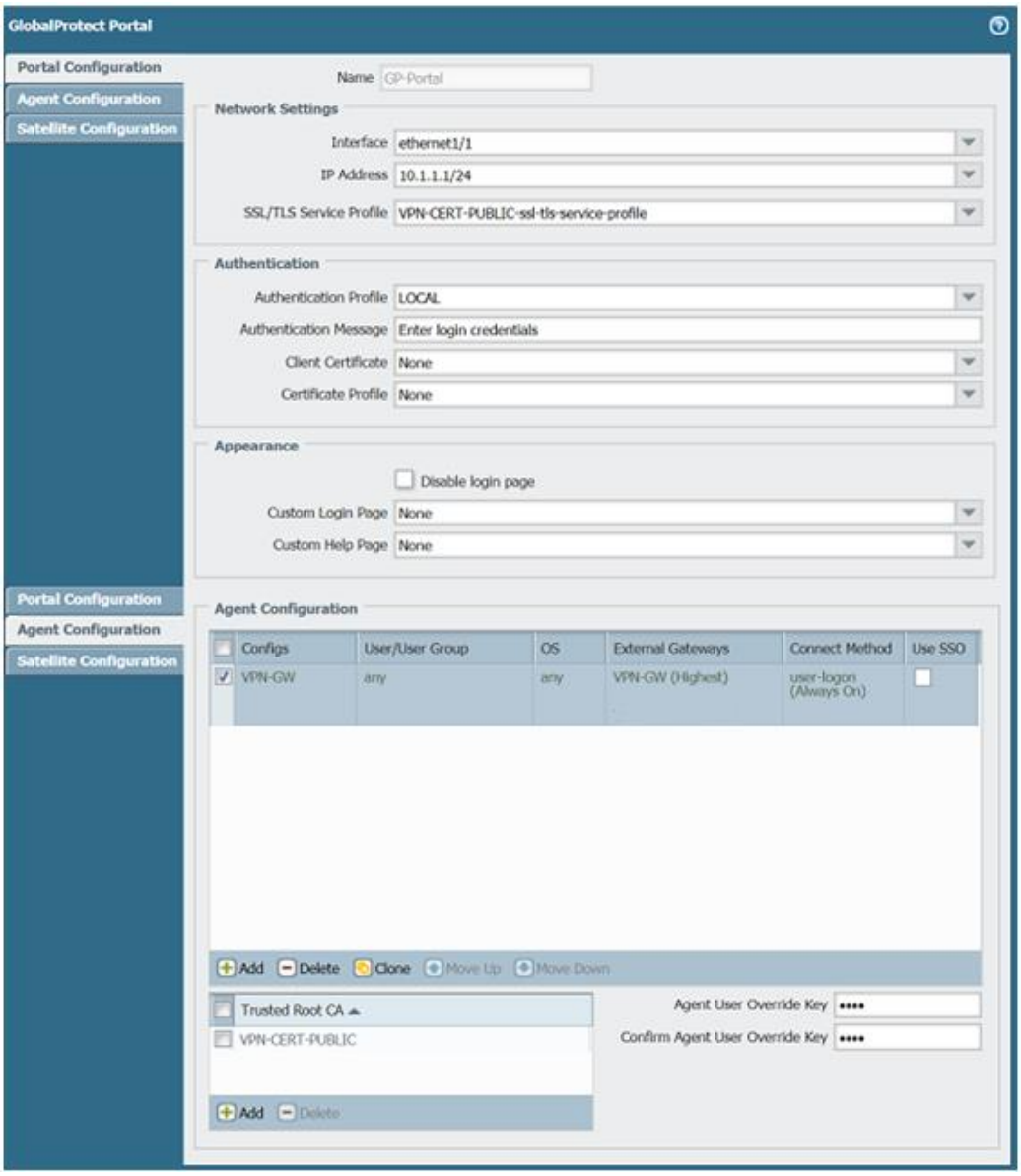


Figure 27. The VPN portal configuration of the firewall

In figure 27, the network settings are chosen from the dropdown menu so that they are equal to outside interface's settings. The settings tells that the VPN portal can be reached from the outside interface. The VPN portal needs a certificate. The certificate is used for encryption. The certificate used in the project was generated by the firewall. The authentication settings tells portal to use local user database to authenticate VPN clients.

The agent configuration defines from which external IP address clients connect. "VPN-GW (Highest)" is configured to be the public IP address of the 4G router connect to the firewall.

The gateway configuration includes network and authentication settings. Figure 27 demonstrates the gateway configuration on the firewall.

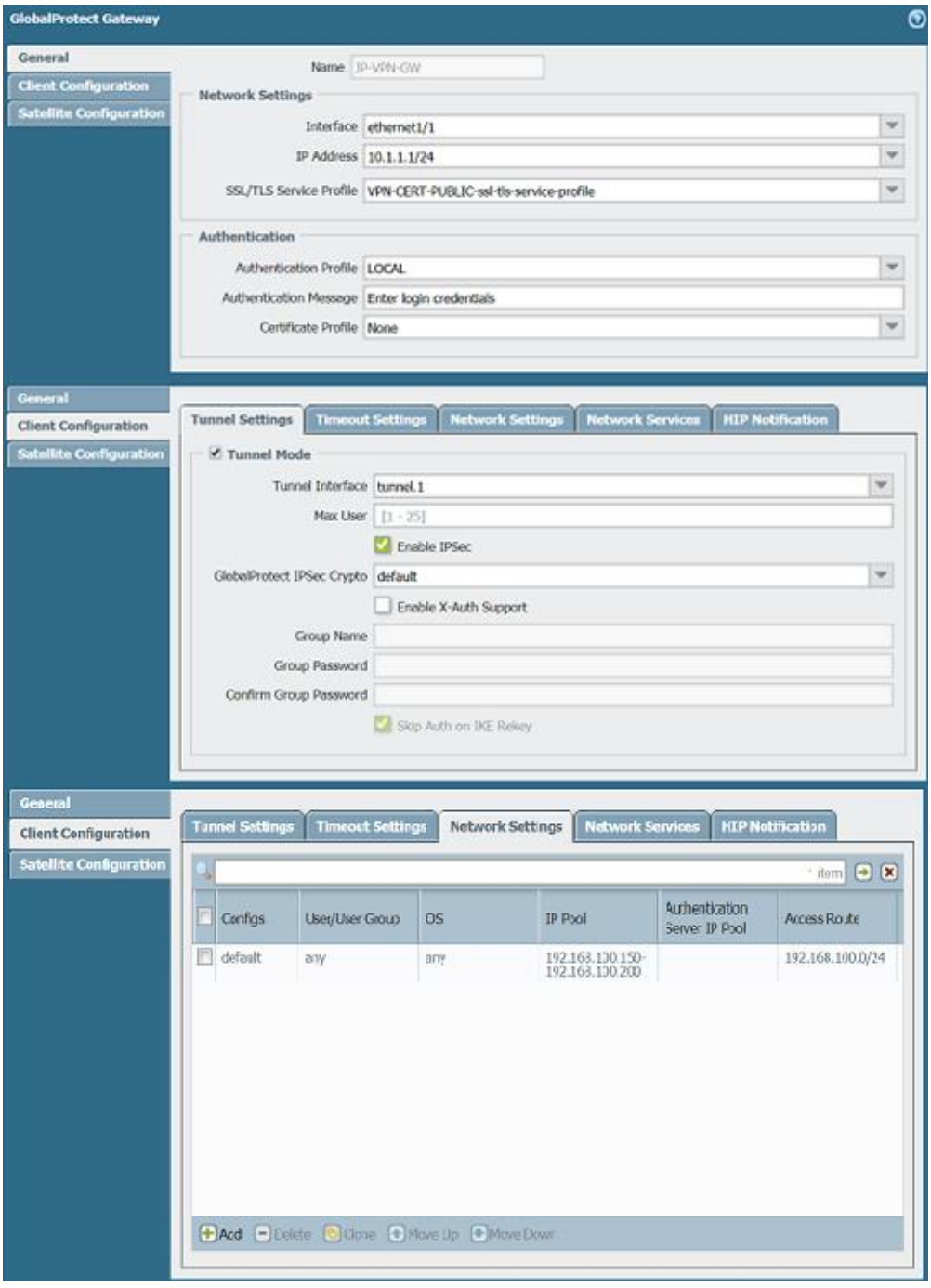
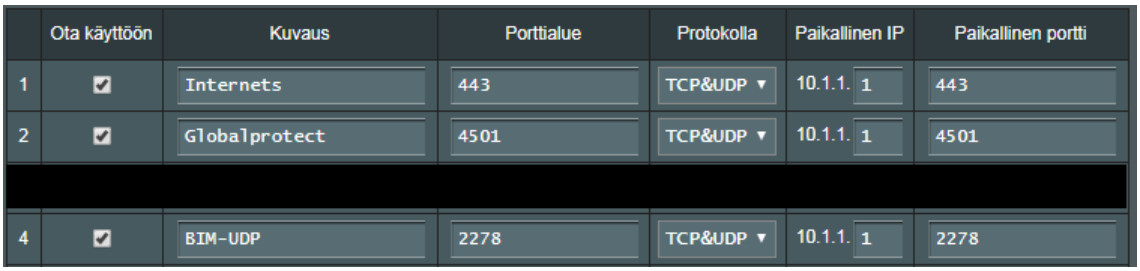


Figure 28. The VPN gateway configuration of the firewall

In figure 28, the gateway general configuration page is similar to the portal general configuration page shown in figure 27. The client configuration page defines the tunnel interface created earlier. The "Enable IPSec" has to be checked for packet authentication and encryption. Client configuration's Network settings are configured because the VPN gateway has to know which IP address can be assigned to the VPN clients. "Access Route" defines the network where the VPN clients are connected.

4.2 4G Router Asus N12 LTE

This 4G Router was located in a rack at Leppävaara campus. The only thing needed to configure to Asus after setting IP addresses was to make port forwarding configurations. Figure 29 shows the ports, which were used for the project.



	Ota käyttöön	Kuvaus	Porttialue	Protokolla	Paikallinen IP	Paikallinen portti
1	☑	Internets	443	TCP&UDP	10.1.1. 1	443
2	☑	Globalprotect	4501	TCP&UDP	10.1.1. 1	4501
4	☑	BIM-UDP	2278	TCP&UDP	10.1.1. 1	2278

Figure 29. Ports forwarded to the firewall from the Asus 4G router

Rule 1 and 2 were needed to enable Palo Alto GlobalProtect VPN. Rule 4 was the port, which was used by the thermal cameras to send the data. All the data is forwarded to Palo Alto's outside interface address.

4.3 Ubiqutiti Nanobeam AC 19

Antennas needed to be configured as a station and an access point. Ubiquinti Nanobeams are configured through a web interface called AirOS 7. The configuration was clear and easy. The connection was secured by WPA2-AES encryption.

Figure 30 shows the configuration of both directional antennas.

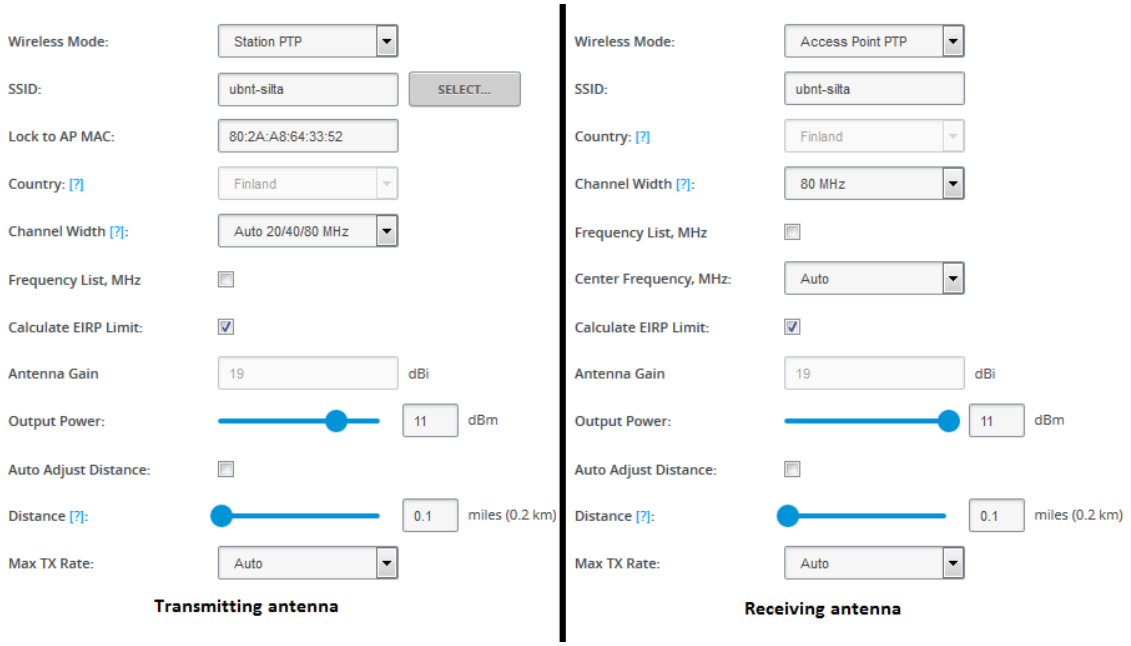


Figure 30. Configuration of both directional antennas

As seen in figure 30, left side is configuration of the antenna which was connecting the thermal cameras to the network and the right side is configuration of the antenna which was connected to the 4G router. The station needs to have the same SSID as the access point. The station is connected to the access point by entering access point's MAC address to "Lock to AP MAC:" field. 11dBm Output power was enough for the tests even with 1.8 km range.

5 Practical test

This chapter explains the practical test by describing the cameras and the networking devices installation and the events during the different days.

Installation

The practical test was done in Suvilahti at the Flow festival 11.-13.8.2017. The Cameras and the network were installed to the festival area on Thursday night. The cameras and the directional antenna was installed on the tower in front of the main stage. Figure 31 shows the tower which was used to install the cameras and the antenna.

Figure 31. General view of the area

In figure 31, the directional antenna is marked with a red circle. Everything was secured with metal wires. Because of the problems on the receiving antenna placement explained in Chapter 3.3 it had to be placed to the festival area. The receiving antenna was installed around 500 meters distance from the main stage. 500 meters might be enough on an urban area to move the 4G connection to another mobile cell. Usually heavily occupied mobile cell could become a problem but in Suvilahti it is not a problem because it is

located on the middle of Helsinki. Through the weekend changes were done caused by many different things such as bad equipment and unusual weather conditions. Figure 32 shows the final configuration of the network.

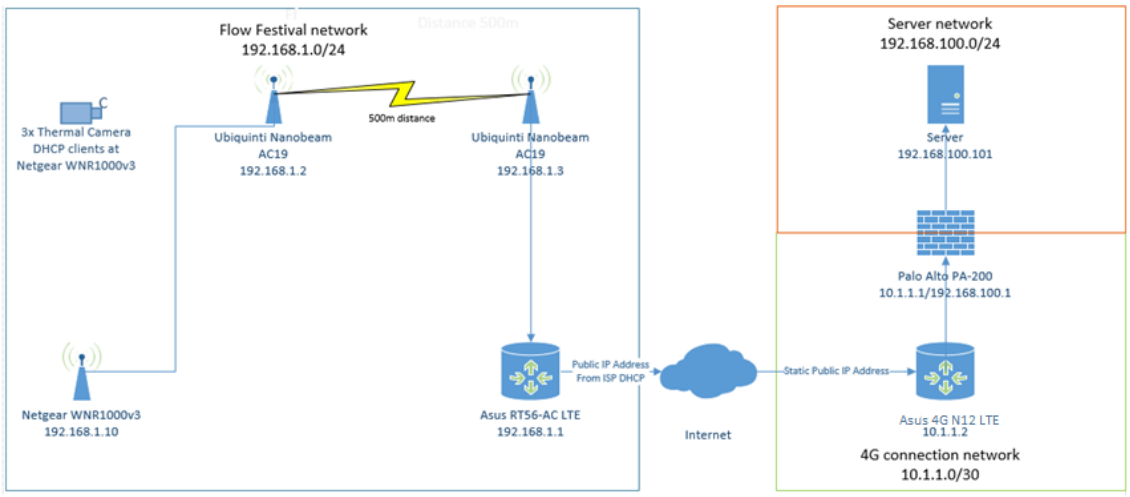


Figure 32. Network topology

In figure 32, the initial networking topology is shown. It presents from left to right how the thermal camera data reached the server.

Friday 11.8.2017

The system was tested on Friday morning. The tests showed that system is working but the image quality was very poor. On a scale of 0-100, the images which were saved to the server were 5. Latencies through the directional antennas were good (1-4ms) but the connection between the WLAN access point and the cameras was unstable. The Image quality problem were pinpointed to the WLAN connection between the cameras and the Netgear WLAN access point which was predicted on the planning. Locating the WLAN access point on the bottom of the tower was a bad idea. There was no time to raise the access point to the top of the tower because gates were opened and the audience came to the area. At night, the connection went down for an unknown reason.

Saturday 12.8.2017

On Saturday morning, the WLAN access point was risen to the tower to the cameras. The connection was down because someone had kicked the power cable. When the

cable was attached to the power source the system went up. The 4G gateway had to be restarted because it was shut down because of inactivity caused by other site's power loss. The connection was still unstable. The image quality went up when RTS threshold value was set to 0 (Explained in Chapter 2.2) on the access point. Now the image quality was 40-70 which is acceptable because the images can be assembled together with image processing.

In the evening, the biggest storm for many years hit Finland and power went down from multiple areas in the metropolitan area. One of these places was Leppävaara. Fuses had cut the power down. After putting power switches back on system restarted and functioned as it should. The system still was not up so there was something on the festival area.

Sunday 13.8.2017

On Sunday morning, the festival site system was damage checked. The system was unaffected by the storm. The cameras and network equipment were on their places thanks for secure attachment. Figure 33 shows the cause of the connection problems.

Figure 33. Cause of connection problems

Figure 33 shows the connection problem, which was caused because light technicians had cut tower's RJ45 cable. There was not a long cable or a repair kit available before the audience comes in. The technicians told that they cut the cable because no one has not told them why it was there. The backup plan was to bring battery a powered 4G dongle and attach it to the bottom of the tower. Unfortunately, the 2.4GHz WLAN band was too occupied at the time of the main event thus the images worth capturing were not taken.

6 Results

This chapter describes the results of the project.

Network

Metropolia's project was not about creating a functioning network to a festival area but it was necessary to make a successful practical test. The network proved to be a working concept whose performance could be improved by the results of the practical test.

Thermal camera images

As a result from the weekend, the thermal cameras recorded images from the tower. Figure 34 shows two slightly processed images from the thermal cameras.

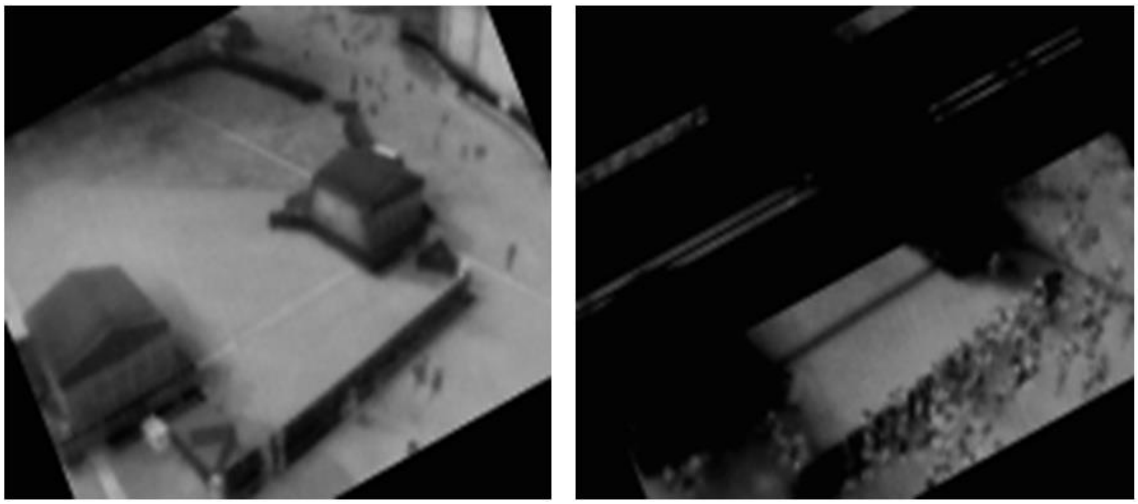


Figure 34. Slightly processed thermal camera images

In Figure 34, the black stripes on the right image are the result of the poor connection between the access point and the camera. The images show clearly that people can be seen from the images. Computer programs could be used to analyze amounts and behavior of people from the images.

7 Improvements

Chapter 7 provides suggestions to improve the overall success for future thermal camera testing including suggestions for networking and project handling.

7.1 Networking improvements

The 2.4GHz WLAN technology was not a satisfying method to send live images in the crowded area. For future events the cameras needs to another transfer method. The safest method is to put wired interfaces on the camera, which was not easily achievable because of the platform used for the cameras. Because the cameras were on the same tower a switch could have been brought up to connect all the cameras to the network. Some wireless methods to test could be 5GHz WLAN and priority SIM-cards from the Rescue Department or another authority.

The Asus 4G router from the Flow Festival network in figure 30 needs to be replaced with a router, which supports fault tolerance protocols. The fault tolerance protocols are designed for example to switch between networking interfaces if the other cannot reach outer network. For an extra layer of security it would be preferred to have site-to-site VPN capable router because then the traffic is encrypted for the whole time. Another option would be to keep the existing 4G router and place a similar Palo Alto firewall to the festival area. The firewall also would support site-to-site VPN.

Placing the receiving end antenna proved to be challenging. The problem was that there was not any line of sight positions for possible receiving end spots. Another pair of directional antennas would have solved the problem because they can be configured in-line. One pair could go around an obstacle and the other pair connect to the receiving end. A more optimal method would be to point place the receiving directional antenna near to the festival network center. The receiving end could be connected to the wired network and privacy could be achieved assigning a private VLAN for the camera network.

7.2 Project handling improvements

The network was a crucial part to make a successful practical test. The project should have budgeted more money to the networking equipment instead of keeping a "let's go what we have" mentality. Five thermal cameras were bought. Only four were placed to the festival area and only two cameras sent the thermal images during the weekend because of the bad connection between the cameras and the access point. Money used

to one camera should have been used to buy a capable access point. A more advanced access point could have made a big difference to the results.

From administrative purposes, every stakeholder needs to know about the project. The project collaborated with a group, which oversaw setting up and maintaining the area's structures but minor groups were not acknowledged and informed. Sunday's data was lost because a group of light technicians did not know what was installed to the tower. Cutting the wire without asking anyone was not obviously the best option but this could have been avoided by telling everyone about the project.

8 Conclusions

Overall, the project did not bring the excepted success but it was not a complete failure either. Due to the poor connection between the cameras and other misfortunes only 8 hours of useful data was collected during the weekend. However, the goal for the project was to prove that thermal cameras can be used for monitoring people on the crowded areas. The data and knowledge of this project are going to be used to generate more advanced systems to provide security and marketing applications with the thermal cameras. The project goals did not have image processing. Image processing is a big project, which could be the subject of another thesis.

The project included lots of planning, a practical test and it achieved concrete results. From the learning aspect ,the fact that everything did not go according to the plans was better compared to the situation where everything went as planned. It was a fairly big project with many learnings from the project management and engineering perspective.

References

1 OSI & TCP/IP models. Online material. < http://study-ccna.com/osi-tcp-ip-models/ />. Accessed 12.10.2017.

2 Introduction to Networks - 3.1.1.4 Message Formatting and Encapsulation. Online material. <https://static-course-sets.s3.amazonaws.com/ITN51/en/index.html#3.1.1.4/>. Accessed as 12.10.2017, through Cisco Networking Academy.

3 Intoduction to Networks - 4.3.1.1 The Data Link Layer. Online material. <https://static-course-sets.s3.amazonaws.com/ITN51/en/index.html#4.3.1.1/>. Accessed as 12.10.2017, through Cisco Networking Academy.

4 Standard Group MAC Addresses. Online material < http://standards.ieee.org/develop/regauth/tut/macgrp.pdf>. Accessed 12.10.2017.

5 Introduction to Networks - 5.3.2.1 Introduction to ARP. Online material. <https://static-course-sets.s3.amazonaws.com/ITN51/en/index.html#5.3.2.1/>. Accessed as 12.10.2017, through Cisco Networking Academy.

6 Introduction to Networks - 6.1.1.1 The Network Layer. Online material. <https://static-course-sets.s3.amazonaws.com/ITN51/en/index.html#6.1.1.1/>. Accessed as 12.10.2017, through Cisco Networking Academy.

7 Introduction to Networks - 6.2.2.2 IPv4 Router Routing Table. Online material. <https://static-course-sets.s3.amazonaws.com/ITN51/en/index.html#6.2.2.2/>. Accessed as 12.10.2017, through Cisco Networking Academy.

8 Introduction to Networks - 9.0.1.1 Transport Layer. Online material. <https://static-course-sets.s3.amazonaws.com/ITN51/en/index.html#9.0.1.1/>. Accessed as 12.10.2017, through Cisco Networking Academy.

9 The Used Datagram Protocol (UDP). Online material. <http://www.erg.abdn.ac.uk/users/gorry/course/inet-pages/udp.html/>. Accessed 12.10.2017.

10 Introduction to Networks - 9.2.1.2 TCP Connection Establishment. Online material. <https://static-course-sets.s3.amazonaws.com/ITN51/en/index.html#9.2.1.2/>. Accessed as 12.10.2017, through Cisco Networking Academy.

11 Introduction to Networks - 9.2.1.3 TCP Session Termination. Online material. <https:// static-course-sets.s3.amazonaws.com/ITN51/en/index.html#9.2.1.3/>. Accessed as 12.10.2017, through Cisco Networking Academy.

12 Introduction to Networks - 9.1.2.4 UDP Header. Online material. < https://static-course- as sets.s3.amazonaws.com/ITN51/en/index.html#9.1.2.4/>. Accessed 12.10.2017, through Cisco Networking Academy.

13 Introduction to Networks - 10.0.1.1 Chapter 10: Application Layer. Online material. <https://static-course- as sets.s3.amazonaws.com/ITN51/en/index.html#10.0.1.1/>. Accessed 12.10.2017, through Cisco Networking Academy.

14 Jääskeläinen, Ville. 2016. Local Area Network. Lecture handout. Metropolia University of Applied Sciences.

15 Kodin ja toimiston säteilevät laitteet. Online material. <http://www.stuk.fi/aiheet/kodin-ja-toimiston-sateilevat-laitteet/langaton-lahiverkko/>. Accessed 14.10.2017, through Cisco Networking Academy.

16 RTS Thresholds in Wireless networks. Online material. < https://sites.google.com/site/embeddedsystesting/wireless-protocols-and-basics-of-wireless-protocols-wlan-802-11a-b-g-n/what-is-rts-threshold-in-wireless/>. Accessed 10.10.2017.

17 Routing and Switching Essentials - 11.1 NAT Operation. Online material. <https://static-course- as sets.s3.amazonaws.com/RSE503/en/index.html#11.1/>. Accessed 7.10.2017, through Cisco Networking Academy.

18 Configuring Network Address Translation and Static Port Address Translation to Support an Internal Web Server. Online material. <https://www.cisco.com/c/en/us/support/docs/long-reach-ethernet-lre-digital-subscriber-line-xdsl/asymmetric-digital-subscriber-line-adsl/12905-827spat.html/>. Accessed 7.10.2017.

19 Routing and Switching Essentials - 9.1 IP ACL Operation. Online material. <https://static-course- as sets.s3.amazonaws.com/RSE503/en/index.html#9.1/>. Accessed 7.10.2017, through Cisco Networking Academy.

20 Connecting Networks - 7.1.1.1 Introducing VPNs. Online material. <https://static-course- as sets.s3.amazonaws.com/CN503/en/index.html#7.1.1.1/>. Accessed 7.10.2017, through Cisco Networking Academy.

21 Kurki, Jouko. Current status and evolution of Wireless networks. Lecture handout. Metropolia University of Applied Sciences.

Thermal Cameras

Thermal cameras were small units capable of capturing and sending thermal images to network. At the practical test there were four cameras. The thermal cameras were planned and built by other Metropolia's student whose responsibility was to capture thermal images and send them to remote location for later analyzing.
The thermal cameras were built into Raspberry Pi casing. Their main parts were Lepton V3 camera module and ESP-8266 microcontroller. The camera module resolution was 160x120 pixels hence it was calculated that the optimal operation height was 10-30 meters. The microcontroller had built-in WLAN adapter which was used to send the data to the network. 2.4GHz WLAN needed to be used because these microcontrollers didn't have RJ45 adapter or 5GHz WLAN. The WLAN adapters weren't configurable.

Thermal cameras in theory are great audience monitor tools. They aren't affected by light conditions and people can’t be identified from thermal images thus data is anonymous and people privacy is safe.